Concerning point V

Reasoned statement with regard to novelty, inventive step, or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents in the present notification:

D1: EP 1 063 811 A (HITACHI EUROP LTD) December 27, 2000 (12-27-2000)
D2: DE 25 53 897 C (SIEMENS AG) January 4, 1979 (01-04-1979)
D3: DE 12 06 011 B (EUROP HANDELSGES ANST) December 2, 1965 (12-02-1965)

1. The present application does not meet the conditions set forth in PCT Article 33(1), as the subject of claims 1-8, 10-19, 21 and 22 do not involve an inventive step as defined by PCT Article 33(3).

2. Document D1, which is considered to be the closest prior art to the subject of claim 1, describes a method for encrypting and decrypting a piece of information (p. 2, l. 3-5); said information being represented by a string of symbols; said symbols being included in a set of symbols hereinafter called the alphabet; said method implementing a pseudo-random generator (p. 4, l. 39-40) that provides a sequence of values hereinafter called a random sequence (p. 4, l. 39-40), the values forming said random sequence being included in a set hereinafter called the random value space; said pseudo-random generator being able to be initialized, prior to utilization and the provision of said random sequence, by means of a string of numbers hereinafter called the initialization key (p. 4, l. 48, "nonce N"); said initialization key determining the random sequence that will be provided by said pseudo-random generator, so that after a subsequent initialization using the same initialization key, the sequence of values provided will be the same as it was after the first initialization; said pseudo-random generator having the advantage that the knowledge of said sequence of values does not make it possible to discover said initialization key within a reasonable amount of time (p. 2, l. 56-58); said method comprising three preliminary steps:

- the preliminary step of defining a set, called the mask alphabet, formed of all or some of the elements in the random value space (p. 5, l. 49-58, the mask alphabet is formed by the elements of $GF(2^b)$ **other than 0**),
- the preliminary step of assigning a permutation of said message alphabet

to each element of said mask alphabet (p. 5, l. 53, the permutation in the example of Document D1 is the **multiplication** in GF(2^b); said three preliminary steps being performed once and for all prior to the first implementation of said method; the implementation of said method, in order to perform the operation of encrypting a piece of information to be encrypted, comprising the following preliminary steps:

- the step of acquiring a string of numbers hereinafter called the primary encryption key (p. 4, l. 39-40, "encryption key K"),
- the step of constructing said initialization key from all or part of said primary encryption key (p. 4, l. 52-57);
- the step of initializing said pseudo-random generator using said initialization key (p. 5, l. 3-4);

said method consisting of selecting, one after another, the symbols composing said information to be encrypted, and of encrypting each of the symbols thus selected (p. 5, l. 3-4) by applying the following operations to it:

- the step of reading the next value in the random sequence provided by said pseudo-random generator (p. 6, l. 3-4, "the block A(i) is tested"),
- if the value read in the preceding step is not an element of said mask alphabet, the step of reiterating the preceding step until an element of said mask alphabet is obtained (p. 6, l. 4-5, if the value of the block is 0, the next block is chosen), the element of said mask alphabet determined in the preceding step will hereinafter be called the mask element,
- the step of selecting the permutation of the message alphabet assigned to said mask element specified in the preceding step (p. 5, l. 49-56),
- the step of applying the permutation of the message alphabet selected in the preceding step to said selected symbol (p. 5, l. 49-56),
- the step of replacing said selected symbol with the result of the permutation performed in the preceding step,

these operations having been executed the method moves on to the next symbol in the information to be encrypted, and so on, until all of the symbols in the information to be encrypted have been processed (p. 5, l. 1-2).

Consequently, the subject of claim 1 differs from the teachings of D1 in that the encryption of the symbols composing the information to be encrypted is executed **selectively**. Said selected symbol is modified according to the method disclosed by Document D1 only if it belongs to the message alphabet. On the other hand, if the selected symbol belongs to the control alphabet, it is not modified.

It is well known to one skilled in the art that the encryption of control symbols can cause errors during the subsequent processing of the messages.

The problem that the present invention proposes to solve may therefore be considered to be to make it possible to subsequently process the messages without errors.

The solution proposed in claim 1 of the present application is not considered to be inventive (PCT Article 33(3)) for the following reasons:

It has long been known by one skilled in the art that **selective encryption** by **omitting the control symbols** solves the potential problems during the subsequent processing of the messages (see for example documents D2 and D3, the important passages being specified in the International Search Report). Consequently, the inclusion of this characteristic in the method described in document D1 constitutes, for one skilled in the art, a normal constructive measure for solving the problem posed. Moreover, the preliminary step of dividing the alphabet into two separate parts, one of said parts being called the control alphabet and being composed of symbols designated not to be modified during encryption, the other of said parts being called the message alphabet and being composed of symbols designated to be potentially modified during decryption, is also part of the method disclosed by D2 (and D3).

Consequently, the characteristics described in documents D1 and D2 would be combined by one skilled in the art, without showing inventiveness, to solve the problem posed. The solution proposed in the independent claim 1 therefore cannot be considered to involve an inventive step (PCT Article 33(3)).

1.2 The same argument applies *mutatis mutandis* to the subject of the corresponding independent claim 12, which therefore is not inventive either.

2. DEPENDENT CLAIMS 2-8, 10, 11, 13-19, 21 and 22

Claims 2-8, 10, 11, 13-19, 21 and 22 do not contain any characteristics which, when combined with the characteristics of any

claim to which they refer, satisfy the requirements of the PCT with regard to inventive step (PCT Article 33(3)).